Security Economics and Critical National Infrastructure

Ross Anderson, Shailendra Fuloria
Cambridge University
Computer Laboratory
name.surname@cl.cam.ac.uk

Abstract

There has been considerable effort and expenditure since 9/11 on the protection of 'Critical National Infrastructure' against online attack. This is commonly interpreted to mean preventing online sabotage against utilities such as electricity, oil and gas, water, and sewage – including pipelines, refineries, generators, storage depots and transport facilities such as tankers and terminals. A consensus is emerging that the protection of such assets is more a matter of business models and regulation – in short, of security economics – than of technology. We describe the problems, and the state of play, in this paper. Industrial control systems operate in a different world from systems previously studied by security economists; we find the same issues (lock-in, externalities, asymmetric information and so on) but in different forms. Lock-in is physical, rather than based on network effects, while the most serious externalities result from correlated failure, whether from cascade failures, common-mode failures or simultaneous attacks. There is also an interesting natural experiment happening, in that the USA is regulating cyber security in the electric power industry, but not in oil and gas, while the UK is not regulating at all but rather encouraging industry's own efforts. Some European governments are intervening, while others are leaving cybersecurity entirely to plant owners to worry about. We already note some perverse effects of the U.S. regulation regime as companies game the system, to the detriment of overall dependability.

Introduction

Modern industrial societies are highly dependant on a small number of utilities that provide power, water, and fuel. In times of conflict, attacks are carried out on enemies' generators, transformers, dams and pipelines; during the cold war, for example, the CIA inserted a Trojan into pipeline control software that the Soviets bought covertly, which caused the pumps, turbines and valves to go haywire and resulted in a "the most monumental non-nuclear explosion and fire ever seen from space" in June 1982[1]. More recently, the US-led coalition knocked out much of Iraq's generating capacity in 2003. These attacks can have serious consequences – in Iraq, for example, delays in restoring electric power were a significant factor in the discontent that led to insurrection against the occupying forces.

Terrorist groups have also targeted critical utilities. Perhaps the worst 'near miss' in recent history was an IRA attempt in 1996 to blow up the four electricity substations that supply London with much of its electricity. That project was thwarted by the police and intelligence services (it later turned out that a senior IRA commander was a British agent) but had it succeeded it would have wrecked electricity supplies to the south-east of England for many months[2]. The only comparable incident in a modern city in peacetime was a five-week outage in central Auckland, New Zealand, caused by a cascade of cable failures in 1998. This led to 60,000 of the 74,000 employees in the area having to work from home or from relocated offices, while most of the 6,000 apartment dwellers in the area moved out for the duration[3]. A power outage such as that planned by the IRA, which would have blacked out millions of people and businesses accounting for perhaps a third of Britain's GDP, would have done immense economic damage.

In the late 1990s, some writers started to point out the vulnerability of industrial control systems to online sabotage. Utility control systems have traditionally been designed for dependability and ease of safe use. They used completely private networks and thus their designers gave no thought to authentication or encryption. These networks were typically organised with a star topology, with many sensors and actuators connected to a control centre. Common protocols such as DNP and Modbus enable anyone who can communicate with a sensor to read it, while anyone who can send data to an actuator can give it instructions. But private networks are expensive, and the prospect of orders-of-magnitude cost reductions led engineers to connect control systems to the Internet. The result was that many industrial control systems became insecure without their owners realising this.

The wake-up call came ten years ago when it was realised that critical control systems might be disrupted by sending carefully chosen commands to the right IP address[4]. The concerns have mainly focussed on the energy and water sectors, although very similar systems are in use in railways, manufacturing and elsewhere, and there are separate but comparable issues with telecomms. At the same time, in the late 1990s there was mounting hype about 'information warfare' whose mavens predicted that the combination of computer- and network-based attacks with propaganda would enable combatants to dominate the 'information battlespace' and gain an advantage comparable to that given by air power in previous generations[5].

After 9/11, government agencies and others started thinking systematically about vulnerabilities that might be exploited by hostile states and substate groups do to damage and cause alarm. One of the early fruits of this program was a series of publications in 2003 that collated information on previous incidents of online sabotage. Poster events included both directed malice, such as a wireless attack on a sewage facility in Queensland, Australia, in 2000 by a disgruntled former employee, and the unplanned effects of less directed malice, notably the shutdown of the Davis-Besse nuclear plant in Ohio in 2003 after some of its systems were infected with the Slammer worm. A database of incidents compiled by the British Columbia Institute of Technology revealed that in 2003 there had been 34 confirmed incidents worldwide of online sabotage, with a further 11 pending investigation[6]. A survey of control systems by the Idaho National Laboratory

from 2004–6 revealed numerous vulnerabilities, and from 2006 there has been a growing number of publications describing threats to control systems[7]. For example, the CIA claimed in January 2008 that a cyber-attack had caused a multi-city power outage at an unspecified location outside the USA[8].

As far as we know, no-one has ever been killed by a cyber-terrorist, and this has limited the attention given by the media to the problems. Some people have even remained sceptical about whether online attacks could do real damage. So in March 2007, the Department of Energy's Idaho National Laboratory made a video demonstrating the 'Aurora vulnerability' in which a series of 'on' and 'off' commands are sent to a generator, timed in such a way as to bring it out of phase and thus destroy it. The video was released to the press in September 2007; in it, a large generating set shudders, emits smoke, and then stops[9]. This helped make clear to legislators that the confluence of the private but internally open systems using in industrial control, with open networking standards such as TCP/IP, was creating systemic vulnerabilities.

SCADA security – the protection of systems designed for Supervisory Control and Data Acquisition – thus become a hot topic. The combination of the clear societal importance of a dependable energy and water supply, the evident vulnerability of existing systems, the salience of 'cyber-terrorism' and the societal sensitisation to terrorism since 9/11 have led to increasing amounts of money and regulatory effort being devoted to it. This paper is a first attempt to set out the security-economics issues that arise. It follows a talk on security economics given by the first author at the SCADA Security Scientific Symposium in January 2009 and discussions with the participants there.

Critical Infrastructure: Externalities of Correlated Failure

The first question we might ask is why the government needs to intervene at all. Surely a utility should be sufficiently motivated to protect its own assets against saboteurs – whether old-fashioned ones using dynamite, or new-fangled ones using network hacks?

We already have two common models of market failure leading to information security failure. In platforms like PCs, the combination of network effects, switching costs and low marginal costs lead to dominant-firm markets with a huge first-mover advantage; in the resulting market races, platform vendors appeal to complementers rather than users, leading to locked-in users and defective security[10]. With mobile phones, a complex supply chain leads to the chip IP owner, chip foundry, software platform vendor, network operator and application vendors all trying to dump risk and liability on each other while the end users have little power[11].

Industrial control systems have both lockin and complex supply chains. A utility that builds a plant such as a power station or oil refinery is typically locked into the control-system vendor for at least 25 years; the vendor for its part typically supplies the software for the central control function, plus the systems integration, while purchasing a wide

range of equipment (cabling, sensors, actuators and indeed whole subsystems) from other vendors.

First, the lockin here has nothing to do with network effects; it's physical. The real assets of the North American energy sector are worth over a trillion dollars; control systems at major sites amount for $3–4 billion, while remote field devices add a further $1.5–2.5bn. Absent a catastrophic attack, this investment will be replaced only when it is fully depreciated. The closest model of which we are aware in the security economics literature is the study by Lookabaugh and Sicker of the U.S. cable-TV industry[12]. There, companies that buy a set-top box technology are locked in for a comparable period. The study found that while the financial effects of lockin were generally negotiated away, the effects on innovation could not be, and that this was a factor in cable TV losing ground to other channels of video distribution such as the Internet.

Second, the complex supply chains don't work in quite the same way as with mobile phones. On the one hand, there is a standards problem, and this is less tractable because relationships in the top tier of the industry are less structured. For example, on one project we might find ABB being the lead contractor, and buying subsystems from Honeywell and GE; on another project, Honeywell might lead while ABB and GE subcontract. The many smaller firms that supply specialist sensors, actuators and so on sell into numerous projects with different prime contractors. Thus, while it was possible for Nokia or ARM to push certain security technologies and standards in the mobile-phone world, it's harder in the world of control systems.

But perhaps the largest difference between the world of industrial control and the world of mobile phones (or PCs) is that the customer is far from powerless. The typical purchaser of critical infrastructure is a big utility or energy company, which has a real liability if a plant blows up. So why can't security just be left to them?

We suggest that a useful way to view this is *the large externalities of correlated failure*. If a small terrorist group – a latter-day Timothy McVeigh – were to blow up a single oil refinery, that might cost $1bn: say $500m of damage and $500m of lost profits during rebuilding. The oil company and its insurers could surely cope. However, if a more organised terrorist group – say Al-Qaida – were to blow up six oil refineries, then chaos and petrol rationing would ensue, with significant damage to the economy. For example, Britain suffered a strike by fuel-tanker drivers in 2001 that caused major disruption for weeks; the loss of six oil refineries might have a comparable impact but for a year or more, leading to social costs in the tens or even hundreds of billions.

The oil company does not internalise the social costs of this, so will make the fence high enough only for a $1bn single-incident loss. If the additional risk of a $100bn multiple-incident loss is to be dealt with, the state may have to step in.

Correlated failure can take many forms. It can result from simultaneous targeted attacks, whether physical attacks as planned by the IRA or cyber-attacks; it could also result from untargeted attacks, such as the Slammer worm that shut down the Davis-Besse nuclear

plant; there could be a simultaneous failure, as was feared might happen due to the "millennium bug"; and there are also cascade failures, where a failure of one part of a network shifts more load suddenly to others, causing a series of trips. The Auckland failure was of this type, and they have a long history. Early power systems were independent and served limited areas; interconnecting them meant that local generator failures could be covered more easily, but the net effect was that failures became rarer but larger. For example, the Great Northeastern Blackout of 1965 left more than 25 million people in Ontario and the Northeastern USA without electricity for almost 12 hours[13]. With electricity, too, the social costs of power failure are much higher than the revenue lost by the power company itself. Security of supply is thus a legitimate public interest.

(In passing, we note that the argument for state intervention is similar in some respects to the case for financial regulation. The isolated failure of a single bank would be of little consequence; it's the risk of correlated failure that rightly worries governments. And correlated failures impose large externalities; Lehman's collapse may have cost its CEO Dick Fuld a few hundred million dollars, but it could cost the world economy over a trillion dollars.)

Regulatory Approaches

Many governments now have programmes for critical national infrastructure protection. By no means all do; for example, the French government leaves pretty well alone. But even among those governments that do intervene, there is great diversity of approach. This may create an interesting natural experiment for security economists to observe.

The UK has espoused light-touch regulation. The Centre for the Protection of National Infrastructure (CPNI) is a part of the Security Service (MI5) and operates by bringing together security managers in particular sectors to share experiences and become more discerning customers; these "buyers' clubs" can exert more pressure (and better-directed pressure) on the control system vendors than individual utilities could acting alone.

The USA, on the other hand, has gone for regulation, at least in the electricity sector. The North American Electric Reliability Corporation (NERC) is a self-regulatory organisation but subject to oversight of the US Federal Energy Regulatory Commission (FERC) and the Government of Canada. Its mission is to ensure the reliability of the bulk power system in North America. Ultimate oversight in the USA is by the Department of Energy and the Department of Homeland Security.

NERC approved a set of standards for Critical Infrastructure Protection (CIP) in June 2006; they come into force in 2009 for every firm in North America that acts as a Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator or Load Serving Entity in the bulk power system. NERC-CIP 001 deals with sabotage reporting; it requires responsible firms to keep proper records and report all sabotage events (and disturbances due to them) to the FBI or the RCMP. NERC CIP 002 through 009 cover cyber security.

Security or Reliability?

NERC CIP 002 is about 'Critical Cyber Asset Identification'. Each responsible entity must first identify critical assets and then those cyber assets essential to their operation. Among the critical assets is any generating plant with a 'black start' capacity. This means that it can be brought up to power even if the grid is down. In case of large scale blackouts black start generators are used to bootstrap the power grid. Hydro power stations are a good example of plant with an intrinsic black start capability; the operator merely has to turn a valve to allow the water into the turbines, and the plant will spin up. Nuclear power stations on the other hand do not by default have such a capability; they need an external power source to be safely brought up to criticality. In the middle lie fossil-fuel generators, which may or may not have black-start capability depending on whether or not they have auxiliary diesel generators. An alternative black-start strategy is for a plant to have the ability to remain operating at reduced power levels while disconnected from the grid.

At the Electric Power 2008 conference, it transpired that plant managers were removing black start capability in order to not have to pay for NERC CIP compliance[14]. This carries a clear cost in terms of system-wide reliability. Some transmission operators were removing IP connectivity from their networks, thereby escaping NERC CIP, while leaving dial-up, bluetooth and other serial communications into their networks vulnerable. In fact, one of our informants described NERC CIP as 'a giant exercise in avoidance'!

It might be more charitable to say that the regulatory regime needs some tuning. In the short term, this may involve intervention at other levels; for example PJM, a regional transmission organisation that coordinates wholesale electricity movement from New Jersey down to North Carolina and as far east as Ohio, and operates power markets among more than 500 firms, is considering allowing NERC CIP compliance costs for black start facilities to be recoverable[15]. But in the medium-to-long term, it is not advisable to have continental and regional regulators pulling in different directions.

The lesson to be learned is that security and reliability should be treated together; the proper target of the regulatory process is the sum of the two, namely dependability. The electricity should continue to come out of the wall socket, regardless of the attempts of either Murphy or Satan to interrupt the supply.

Cross-industry differences

In North America, the electricity industry may be closely regulated, but oil and gas are almost totally unregulated, at least at the level of the control systems themselves. In these industries, the pressure comes from the major companies themselves who exert pressure primarily through the tendering and contracting process. There is indirect regulation through Sarbanes-Oxley, which has given some impetus to their information security strategy.

The oil and gas companies also have much stronger risk management. While failures of electricity supply tend to be merely inconvenient (unless they go on for a long time as in Auckland), explosions at oil and gas facilities tend to be expensive, in terms of lives, dollars and publicity. For example, an explosion at BP's Texas City refinery in March 2005 killed 15 workers and injured over 170 others. BP has paid $1.6 billion compensation to victims and has offered to pay a $50m fine. Its CEO retired early. This is by no means an isolated incident; explosions, spills, and other accidents happen regularly costing serious amounts of money. As a result, large oil companies have long embedded safety and security procedures driven by formal risk-management processes[16]. (In fact BP has taken the lead within the industry in preaching the gospel of SCADA security.)

Certification and lifecycle management

The collision between the proprietary world of industrial control systems and the open world of IP-based networking was a root cause of the current problems with SCADA security. The Internet offers huge cost savings over proprietary networks, and – as in other applications such as banking – there was first a rush to use the new technology to save money, then a realisation that a lot would have to be spent on security in order to deal with the suddenly increased risk of remote attacks. Control systems engineers and vendors are therefore now coming into contact with traditional information security mechanisms, such as patch management and Common Criteria evaluations. A number of tensions are becoming evident.

The security-economics literature has many papers on the costs and incentives that drive lifecycle management[17]. However, common platforms either get routinely patched every month (PCs) or else replaced frequently (mobile phones). Control systems may remain in use for decades, and many of their components were never designed for remote upgrade. The costs of taking down (say) a nuclear power plant to patch components may also be very substantial, while some systems require 99.999% availability – which translates into less than 6 minutes downtime per annum. The upshot is that control systems are patched late or not at all. Patch management has thus become contentious, with some firms believing that vulnerability information should not be published, and arguing in favour of a private CERT or even just reporting to the FBI/RCMP as mandated by NERC CIP. (This appears to be particularly the case with firms from a defence background, while firms whose SCADA business evolved from a civil engineering or computing business tend to favour the normal CERT approach.)

Matters are made more complex by the question of what to certify. In respect of legacy systems that cannot feasibly be patched, there used to be a get-out: an 'unless technically infeasible' clause in CIP. That is now being removed, and legacy systems are being protected by firewalls of various kinds. There, a 'normal' approach of frequent upgrades and CERT notification of vulnerabilities may apply to the firewall itself; there is the separate question of the rules applied by the firewall to protect the vulnerable devices behind it. The Department of Homeland Security has taken a step into this debate by

issuing recommended practice for patch management of control systems according to which responsible entities must establish a patch management program dealing with hardware inventory, network mapping, software libraries and operational procedures such as patch testing and incident response[18]. This allows the asset owner to customise their plan to their circumstances, but not to just leave patch management in the 'too hard' file. However, it gives little guidance about prioritisation. The difficulty of establishing good security metrics pervades this field, as it does others; the value-at-risk approach based on annualized loss expectancy does not give hard numbers unless there's adequate loss history, and the proxies used when applying security economics to traditional IT (insurance markets, stock markets and vulnerability markets) give less or no information to the control systems engineer. At least in traditional IT, we are starting to gather statistics on attacks, even although we don't have as many statistics as we'd like[19]; but there have been too few documented cyber-attacks on control systems to give us much guidance.

The move towards Common Criteria certification of protection systems and components will also raise familiar issues. Although control systems security is fundamentally about integrity and availability rather than confidentiality, there is still a multilevel element: the plant safety system should be protected from errors in (or attacks on) the control system, while the control system must in turn must be protected from the everyday systems used by office staff. Multilevel security is hard, and providing high levels of assurance is also hard. At the lower levels of Common Criteria assurance, evaluations are performed by commercial licensed evaluation facilities (CLEFs) – that is, by companies that compete for the vendor's business, giving the vendor every assurance to pick the CLEF that will give its products the easiest ride[20].

What's more, full Common Criteria certification is so slow and expensive that there will be every incentive to resort to shortcuts. The UK banks, for example, have PIN entry devices "Common Criteria evaluated" which means that they were evaluated by a CLEF, but outside the Common Criteria scheme. Such products turned out to be pathetically insecure[21]. The control systems community do not seem to realise how hard security certification can be, and the costs – especially when layered on top of existing safety certification processes – could be very substantial. At present, U.S. regulators are mulling over whether to require control systems to undergo Common Criteria evaluation. NIST produced a Protection Profile for industrial control systems as early as 2004[22]. This isn't the place for detailed technical discussion; we merely warn that there are significant policy issues that need to be thought through before such a step is taken. It is likely to be more expensive, and less helpful, than one might naively think.

And there are many tensions that engineers have still not begun to explore. For example, ease of safe use is a priority in control systems design, and security usability is known to be hard. Will we see conflicts between security and safe usability? As a typical plant operator earns less than $40,000, the 'Homer Simpson' problem is a real one. How do we design security that Homer can use safely?

The Roadmap

Much of the last ten years of control systems security work has been aimed at fixing the vulnerabilities that arose when previously isolated systems were heedlessly connected to the Internet. For many firms that has involved purchasing large numbers of firewalls and encryption devices so as to ensure that the traditional private networks were isolated from the Internet by an "electronic security perimeter" (as NERC CIP 005 puts it). They have thus been reconstituted as virtual private networks. However maintaining this perimeter is hard, and many incentives drive towards 'deperimterisation' (an ongoing debate in the network security community). Component vendors helpfully include new modes of communication; a transformer may now come with bluetooth connectivity and its own web server, so that the engineer doesn't have to get out of his truck in the rain to take meter readings and adjust parameters. As fast as the security engineers can close down unauthorised access points, innovators open them up.

There is thus a growing consensus on the need to move towards a more systematic approach. Control systems should migrate to using protocols that have appropriate security measures built in to support authentication and resist service-denial attacks. There is just no feasible alternative to using commercial-off-the-shelf components in control systems, and the consequences of this have to be dealt with.

The U.S. Departments of Energy and Homeland Security therefore launched in January 2006 a Roadmap to Secure Control Systems in the Energy Sector[23], based on a 2005 workshop with asset owners and operators. Its vision is that within ten years control systems throughout the U.S. energy sector will be able to survive an intentional cyber assault with no loss of critical function in critical applications. It is not limited to engineering new control systems, but encompasses the continuing the protection of surviving legacy systems, understanding strategic threats better, training, information sharing and other support activities. It focusses on critical assets, just like NERC CIP (and this does raise the issue of what happens if a worm like Blaster takes out a lot of unprotected 'non-critical' systems, whose cumulative contribution is critical). A significant number of technical research projects have been funded at various universities and national laboratories. A significant roadmap goal is to sustain the security improvements that this research will make possible. The roadmap acknowledges nine challenges:

- Limited resources are available within businesses to address security needs;
- Cyber security is a difficult business case;
- Limited knowledge, understanding and appreciation of control systems security risks inhibit sector;
- Insufficient sharing of threat and incident information among government and industry entities;
- Effective security-oriented partnerships between government and industry have been difficult to establish;
- Poor coordination among government agencies creates confusion and inefficiencies;

- New regulation may impose requirements beyond the technical capability of legacy systems;
- Highly educated staff with broad skill sets is needed to manage future operations.
- Increasing sophistication of tools used by hackers.

About five of these nine fall with the classical remit of information security economics. It might therefore be appropriate for more of the research budget to be directed towards security economics research rather than purely technical projects. The security engineering community already knows how to do things like crypto, protocols, and access controls; what we don't know how to do is to ensure sustainable implementation and effective use of these technologies in different business environments.

Conclusion

Security is hard. Control systems are hard too. Control systems security will be harder; but most governments now accept that it has to be tackled. Modern societies depend completely on utilities such as electricity, oil, water and sewage, and these systems have become vulnerable to online attack.

In this paper we have looked at the state of play some ten years after this first became an issue, and some three years after the U.S. government took major policy initiatives in the form of the NERC CIP standards and the Roadmap. It is by now clear that control systems security is at least as much a security-economics problem as it is a technical one. Yet the issues are interestingly different from those studied so far by security economists. The lockin is physical rather than based on network effects; a case for government intervention may be made because of the large externalities of correlated failure; existing regulations have led companies to game the system, to the detriment of dependability; established patch management practices conflict with control system realities; a move to Common Criteria certification could be hugely expensive; and different regulatory approaches in the USA and Europe, as well as between different U.S. industries, have created a large natural experiment for security economists to study.

Acknowledgement

The second author's research is funded by ABB. The contents of this article do not necessarily express the views of ABB.

References

1 "The Farewell Dossier", W Safire, New York Times, February 2 2004
2 "Britain Convicts 6 of Plot to Black Out London", W Hoge, New York Times, July 3 1997
3 "Auckland's Power Outage, or, Auckland – Your Y2K Beta Test Site", Peter Gutmann, at www.cs.auckland.ac.nz/~pgut001/misc/mercury.txt
4 "Network Secures Process Control", E.J. Byres, in Tech Magazine, Instrumentation Systems and Automation Society, Research Triangle Park, NC, October 1998
5 'Information Warfare and Security'', D Denning, Addison-Wesley (1999)

6 “The Myths and Facts behind Cyber Security Risks for Industrial Control Systems”, Eric Byres, Justin Lowe, BCIT 2003
7 “Lessons learned from cyber security assessments of SCADA and energy management systems’’, Raymond Fink, David Spencer, Rita Wells, US Department of Energy, Sep 2006, at http://www.us-cert.gov/control_systems/csdocuments.html
8 “CIA Confirms Cyber Attack Caused Multi-City Power Outage”, Alan Paller, SANS Newsbites v 10 no 5, Jan 18 2008
9 “Sources – Staged cyber attack reveals vulnerability in power grid”, Jeanne Meserve, CNN Sep 26 2007, at http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html
10 “Why Information Security is Hard – An Economic Perspective”, Ross Anderson, in Proceedings of ACSAC 2001 pp 358–365
11 ‘Security Engineering -- A Guide to Building Dependable Distributed Systems’, Ross Anderson, Second edition, Wiley 2008
12 “Security and Lock-in”, D Lookabaugh, T Sicker, in ‘Economics of Information Security’ (LJ Camp, S Lewis, eds.) pp 225–246; also at WEIS 2003
13 “The 'Great Northeastern Blackout' of 1965”, CBC Digital Archives, at http://archives.cbc.ca/economy_business/energy/topics/874/
14 “Electric Power 2008 – is NERC CIP Compliance a Game?”, Joe Weiss, Control Global Community, Sep 5 2008, at http://community.controlglobal.com/content/electric-power-2008%E2%80%93-nerc-cip-compliance-game
15 “Black Start Service Working Group – MRC Update”, Jan 15 2009, at www.pjm.com/Media/committees-groups/working-groups/bsswg/20090217/20090217-mrc-update-01-15-09.pdf
16 “Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition”, American Petroleum Institute, October 2004; at http://www.npradc.org/docs/publications/newsletters/SVA_2nd_Edition.pdf
17 See for example the Security Economics Resource Page, http://www.cl.cam.ac.uk/~rja14/econsec.html
18 “Recommended Practice for Patch Management of Control Systems”, Department of Homeland Security, Dec 2008; at http://csrp.inl.gov/Documents/PatchManagementRecommendedPractice_Final.pdf
19 “Security Economics and European Policy'", Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore, ENISA, at WEIS 08, at http://www.ross-anderson.com
20 Anderson, “Security Engineering”, op. cit., Chapter 26
21 “Thinking inside the box: system-level failures of tamper proofing”, Saar Drimer, Steven J. Murdoch, Ross Anderson, University of Cambridge Technical Report TR-711, Feb 2008; at http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-711.html
22 ‘System Protection Profile - Industrial Control Systems’, Ron Melton, Terry Fletcher and Matt Early, NIST 2004; at www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.pdf
23 Roadmap to Secure Control Systems in the Energy Sector, Department of Energy, Department of Homeland Security, January 2008, at http://www.controlsystemsroadmap.net/